Política de Certificado de Assinatura Digital Tipo A3

da Autoridade Certificadora Imprensa Oficial SP para a Secretaria da Receita Federal do Brasil

PC A3 da AC Imprensa Oficial SP RFB

Versão 6.0 - 24 de Julho de 2014

ÍNDICE

Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Imprensa Oficial SP RFB

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A3 da Autoridade Certificadora Imprensa Oficial SP RFB na Infra-estrutura de Chaves Públicas Brasileira.

A estrutura desta PC está baseada no DOC ICP 04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 2527 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.1.2. Não se aplica.

1.1.3. Não se aplica.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

1.2. Identificação

1.2.1. Esta PC é chamada "Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Imprensa Oficial SP RFB" e referida como "PC A3 da AC Imprensa Oficial SP RFB". Esta PC descreve os usos relacionados ao certificado de Assinatura Digital corresponde ao tipo A3 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.3.16.

1.2.2. Não se aplica.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC Subordinada Imprensa Oficial SP RFB (AC Imprensa Oficial SP RFB) no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC Imprensa Oficial SP RFB estão descritos na Declaração de Práticas de Certificação da AC Imprensa Oficial SP RFB (DPC da AC Imprensa Oficial SP RFB).

1.3.2.Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Imprensa Oficial SP RFB para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitaios e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC Imprensa Oficial SP RFB (https://www.certisign.com.br/certisign/repositorios/icp-brasil/autoridades-registro/ac-imesp-rfb):

a) relação de todas as ARs credenciadas, com informações sobre as PC que implementam.

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

d) relação de AR que tenham se descredenciado da cadeia da AC Imprensa Oficial SP RFB, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;

f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICPBrasil, se for o caso.

1.3.2.2. A AC Imprensa Oficial SP RFB mantém as informações acima sempre atualizadas.

1.3.3. Prestador de Serviço de Suporte

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC Imprensa Oficial SP RFB e/ou por intermédio de suas ARs é publicada em serviço de diretório e/ou em página web da AC Imprensa Oficial SP RFB (http://icp-brasil.certisign.com.br/repositorio/ac-imesp-rfb/index.htm.

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas ARs para desempenhar atividade descrita nesta DPC ou nas PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infra-estrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC Imprensa Oficial SP RFB mantém as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Pessoas físicas ou jurídicas inscritas no CPF ou no CNPJ podem ser Titulares de Certificado e-CPF ou e-CNPJ Tipo A3, desde que não enquadradas na situação cadastral de CANCELADA (pessoa física) ou na condição de BAIXADA, INAPTA, SUSPENSA ou CANCELADA (pessoa jurídica), conforme o disposto nos incisos I e II do art. 6° da Instrução Normativa RFB n° 1077, de 29 de Outubro de 2010.

No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Obrigatoriamente, o Responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrado no CNPJ da RFB.

1.3.5. Aplicabilidade

1.3.5.1. Neste item são relacionadas as aplicações para as quais os certificados definidos por esta PC são adequados.

1.3.5.2. Os certificados emitidos pela AC Imprensa Oficial SP RFB no âmbito desta PC também podem ser utilizados para confirmação de identidade do titular em aplicações como Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas; para cifração de chaves de sessão, assinatura de documentos eletrônicos e verificação da integridade de informações transmitidas eletronicamente.

Os certificados digitais e-CPF e e-CNPJ são utilizados para identificação do Contribuinte e acesso ao Sistema Interativo de Atendimento Virtual (Receita 222), para as opções de atendimento, via internet, disponibilizadas pela RFB.

1.3.5.3. A AC Imprensa Oficial SP RFB leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, freqüência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.3.5.4. Os certificados emitidos pela AC Imprensa Oficial SP RFB no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. Não se aplica.

1.3.5.6. O "Termo de Titularidade", no caso de certificados de pessoas jurídicas, equipamentos ou aplicações, disponibilizados pela da AR que recebe e valida o pedido de emissão de certificado poderá limitar as aplicações para as quais são adequados os certificados de assinatura – tipo A3 emitidos pela AC Imprensa Oficial SP RFB, determinando restrições ou proibições de uso destes certificados.

1.4.Dados de Contato

Nome: Imprensa Oficial do Estado SA IMESP

Endereço: Rua da Mooca, 1921 – Mooca – São Paulo, SP

Nome: João Paulo Foini

Telefone: (11) 2799-9800 / (11) 2799-9782
E-mail: certificacao@imprensaoficial.com.br

2. DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SP RFB.

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SP RFB.

3.1.Registro Inicial

3.1.1.Disposições Gerais

3.1.2.Tipos de nomes

3.1.3.Necessidade de nomes significativos

3.1.4.Regras para interpretação de vários tipos de nomes

3.1.5.Unicidade de nomes

3.1.6. Procedimento para resolver disputa de nomes

3.1.7.Reconhecimento, autenticação e papel de marcas registradas

3.1.8.Método para comprovar a posse de chave privada

3.1.9.Autenticação da identidade de uma organização

3.1.9.Autenticação da identidade do indivíduo

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

3.1.9.2 Informações contidas no certificado emitido para um individuo

3.1.10.Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.2 Documentos para efeitos de identificação de uma organização

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.11.Autenticação da identidade de um equipamento ou aplicação

3.1.10.1. Disposições Gerais

3.1.10.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.1.10.3. Informações contidas no certificado emitido para um equipamento ou aplicação

3.2.Geração de novo par de chaves antes da expiração do atual

3.3.Geração de novo par de chaves após revogação

3.4.Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SP RFB.

4.1.Solicitação de Certificado

4.2.Emissão de Certificado

4.3.Aceitação de Certificado

4.4.Suspensão e Revogação de Certificado

4.4.1.Circunstâncias para revogação

4.4.2.Quem pode solicitar revogação

4.4.3.Procedimento para solicitação de revogação

4.4.4.Prazo para solicitação de revogação

4.4.5.Circunstâncias para suspensão

4.4.6.Quem pode solicitar suspensão

4.4.7.Procedimento para solicitação de suspensão

4.4.8.Limites no período de suspensão

4.4.9.Freqüência de emissão de LCR

4.4.10.Requisitos para verificação de LCR

4.4.11.Disponibilidade para revogação ou verificação de status *on-line*

4.4.12.Requisitos para verificação de revogação *on-line*

4.4.13.Outras formas disponíveis para divulgação de revogação

4.4.14.Requisitos para verificação de outras formas de divulgação de revogação

4.4.15.Requisitos especiais para o caso de comprometimento de chave

4.5.Procedimentos de Auditoria de Segurança

4.5.1.Tipos de eventos registrados

4.5.2.Freqüência de auditoria de registros (*logs*)

4.5.3.Período de retenção para registros (*logs*) de auditoria

4.5.4.Proteção de registro (*log*) de auditoria

4.5.5.Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

4.5.6.Sistema de coleta de dados de auditoria

4.5.7.Notificação de agentes causadores de eventos

4.5.8.Avaliações de vulnerabilidade

4.6.Arquivamento de Registros

4.6.1.Tipos de registros arquivados

4.6.2.Período de retenção para arquivo

4.6.3.Proteção de arquivo

4.6.4.Procedimentos para cópia de segurança (*backup*) de arquivo

4.6.5.Requisitos para datação (*time-stamping*) de registros

4.6.6.Sistema de coleta de dados de arquivo

4.6.7.Procedimentos para obter e verificar informação de arquivo

4.7.Troca de chave

4.8.Comprometimento e Recuperação de Desastre

4.8.1.Recursos computacionais, *software*, e dados corrompidos

4.8.2.Certificado de entidade é revogado

4.8.3.Chave de entidade é comprometida

4.8.4.Segurança dos recursos após desastre natural ou de outra natureza

4.8.5.Atividades das Autoridades de Registro

4.9.Extinção dos serviços de AC, AR ou PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SP RFB.

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante, apresentados pelo browser Microsoft ou Netscape.

A chave privada é exportada e armazenada em mídia externa – Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou hardware criptográfico aprovado pelo CG da ICPBrasil.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A3.

6.1.1.5. O usuário deve assegurar que a chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6. O meio de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. O meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que estes dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado emitido pela AC Imprensa Oficial SP RFB e descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil.

6.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular do certificado, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física.

6.1.2. Entrega da chave privada à entidade titular do certificado

Item não aplicável.

6.1.3. Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado AC Imprensa Oficial SP RFB, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

6.1.4. Disponibilização de chave pública da AC para usuários

A AC Imprensa Oficial SP RFB disponibiliza o seu certificado e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil no padrão PKCS#7, através de endereço Web: http://icp-brasil.certisign.com.br/repositorio/ac-imesp-rfb/index.htm.

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Imprensa Oficial SP RFB é de 1024 bits para as hierarquias V0 e V1 e de 2048 bits para as hierarquias V2.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 da ICP-Brasil está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BARSIL [1].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (Cryptographic Module Validation Program) do NIST (National Institute of Standards and Technology).

6.1.8. Geração de chave por hardware ou software

A geração das chaves criptográficas do Certificado Tipo A3 desta PC, é realizada por hardware criptográfico aprovado pelo CG da ICP-Brasil.

6.1.9. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

Os pares de chaves correspondentes aos certificados emitidos pela AC Imprensa Oficial SP RFB podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

6.2. Proteção da Chave Privada

6.2.1. Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (Federal Information Processing Standards) 140-1, 140-2 ou outro de conteúdo semelhante a um destes citados.

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2. A AC Imprensa Oficial SP RFB não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC Imprensa Oficial SP RFB não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

6.2.5.2. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

O titular de certificado de e-CPF ou e-CNPJ deve obrigatoriamente utilizar senha para a proteção de sua chave privada, de acordo com o art. 5° da Instrução Normativa RFB N° 222, de 1077, de 29 de Outubro de 2010.

6.2.8. Método de desativação de chave privada

O titular de certificado pode definir procedimentos necessários para a desativação de sua chave privada.

6.2.9. Método de destruição de chave privada

O titular de certificado pode definir procedimentos necessários para a destruição de sua chave privada.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas dos titulares de certificados de assinatura digital emitidos pela AC Imprensa Oficial SP RFB permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC Imprensa Oficial SP RFB são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de Assinatura Digital Tipo A3 da AC Imprensa Oficial SP RFB é de 5 (cinco) anos.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade.

O equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

6.5.2. Classificação da segurança computacional

Item não aplicável.

6.6. Controles Técnicos do Ciclo de Vida

A AC Imprensa Oficial SP RFB desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC Imprensa Oficial SP RFB utiliza um modelo clássico espiral no desenvolvimento dos sistemas. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC Imprensa Oficial SP RFB utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC Imprensa Oficial SP RFB provêem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Imprensa Oficial SP RFB.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC Imprensa Oficial SP RFB verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a

natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC Imprensa Oficial SP RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado está em conformidade com o padrão de segurança FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2), utilizando o algoritmo RSA.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC Imprensa Oficial SP RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. Número de versão

Os certificados emitidos pela AC Imprensa Oficial SP RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas pela AC Imprensa Oficial SP RFB e sua criticalidade.

7.1.2.2. Extensões Obrigatórias

Os certificados emitidos pela AC Imprensa Oficial SP RFB obedecem a ICP - Brasil, que define como obrigatórias as seguintes extensões:

a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Imprensa Oficial SP RFB;

b) **Key Usage,** crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;

c) **Certificate Policies**, não crítica contém:

- O OID desta PC: 2.16.76.1.2.3.6;

• Os campos policyQualifiers contém o endereço *Web* da DPC AC Imprensa Oficial SP RFB: (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP_RFB/DPC_AC_IMESP_RFB.pdf) .

d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC Imprensa Oficial SP RFB:

Para certificados emitidos até 31/01/2011:
http://icp-brasil.certisign.com.br/repositorio/lcr/ACIMESPRFBG2/LatestCRL.crl
http://icp-brasil.outralcr.com.br/repositorio/lcr/ACIMESPRFBG2/LatestCRL.crl
http://repositorio.icpbrasil.gov.br/lcr/RFB/ACIMESPRFBG2/LatestCRL.crl

Para certificados emitidos a partir de 01/01/2012:
http://icp-brasil.certisign.com.br/repositorio/lcr/ACImprensaOficialSPRFBG3/LatestCRL.crl
http://icp-brasil.outralcr.com.br/repositorio/lcr/ACImprensaOficialSPRFBG3/LatestCRL.crl
http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACImprensaOficialSPRFBG3/LatestCRL.crl

e) **Authority Information Access**, não crítica: contem o endereço de acesso aos certificados da cadeia de certificação através do link: http://icp-brasil.certisign.com.br/repositorio/certificados/AC_IMESP_RFB_G3.p7c e o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (On-line Certificate Status Protocol- OCSP): http://ocsp.certisign.com.br.

f) **basicConstraints**, não crítica: contém o campo cA=False.

7.1.2.3. Os certificados emitidos pela AC Imprensa Oficial SP RFB possuem a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:
a) Para certificado de pessoa física:
a.1) 4 (quatro) campos otherName, obrigatórios, contendo nesta ordem:
i· OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS,PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG)

do titular; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

ii· OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.

iii· OID = 2.16.76.1.3.5 e conteúdo nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 posições subseqüentes, o município e a UF do Título de Eleitor.

a.2) campo rfc822Name contendo o endereço e-mail do titular do certificado.
a.3) campo otherName, não obrigatório, contendo:

i· OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN).

b) Para certificado de pessoa Juridica:
b.1) 5 (cinco) campos otherName, contendo, nesta ordem:
i· OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva Unidade da Federação;

ii· OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica;

iii· OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

iv. OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

b.2) campo rfc822Name contém o endereço e-mail do responsável pela Pessoa Jurídica titular do certificado.

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) campos otherName, obrigatórios,contendo, nesta ordem:

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;
ii. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;
iii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;
iv. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

Quando certificados de equipamento forem emitidos para servidores de Domain Controller, adicionalmente irão conter:
c.2) campo otherName, contendo:
OID = 1.3.6.1.4.1.311.25.1 contendo o identificador (Globally Unique Identifier - GUID) do Domain Controller;

c.3) campo DNS Name, contendo o nome do domínio.

c.4) campo rfc822Name contém o endereço e-mail do responsável pelo certificado ou da pessoa jurídica, em caso de email corporativo.

7.1.2.4. Os campos otherName, definidos como obrigatórios, estão de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING;

b) Quando os números de NIS (PIS, PASEP ou CI), RG, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor/UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Titulo de Eleitor;

d) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

e) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre municípios e UF do Título de Eleitor;

f) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais, com exceção do campo UPN que utiliza caracteres especiais;

g) O campo UPN é opcional, caso não seja usado o OID não é incluído no certificado.

7.1.2.5. Não se Aplica

7.1.2.6. Os outros campos que compõem a extensão "Subject Alternative Name" podem ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7. A AC Imprensa Oficial SP RFB implementa a extensão "Extended Key Usage", não crítica, contendo o valor "server authentication" (OID 1.3.6.1.5.5.7.3.1), e podendo conter os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2) e/ou "Netscape SGC" (OID 2.16.840.1.113730.4.1) e/ou "Microsoft SGC" (OID 1.3.6.1.4.1.311.10.3.3) para certificados de equipamento, o valor "client authentication" (OID 1.3.6.1.5.5.7.3.2) e podendo conter os valores "code signing" (OID 1.3.6.1.5.5.7.3.3) e/ou "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4) e/ou "OCSPSigning" (OID 1.3.6.1.5.5.7.3.9) para certificados de aplicação e os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2), "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) e podendo conter o valor "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2), quando for utilizado o campo "UPN" na extensão "Subject Alternative Name", para certificados de pessoa jurídica e pessoa física.

7.1.3.Identificadores de algoritmo

Os certificados emitidos pela AC Imprensa Oficial SP RFB são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas hierarquias V0 e V1, e algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) nas hierarquias V2 conforme o padrão PKCS#1.

7.1.4.Formatos de nome

O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594.

Cada PC implementada pela AC Imprensa Oficial SP RFB especifica corretamente os formatos dos certificados gerados e das correspondentes LCRs. As PC incluem informações sobre os padrões adotados, seus perfis, versões extensões.

e-CPF:

O conteúdo do DN apresenta-se da seguinte forma para os certificados de Pessoa Física:

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-CPF A3

OU = <Domínio do certificado>

OU = <Identificação da AR>

CN = <Nome da Pessoa Física> <:> <número de inscrição no CPF>

Onde:

O Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com cumprimento máximo de 52 (cinqüenta e dois) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.

Um "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Um segundo "OU" com conteúdo variável, informando no campo domínio a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor. Caso esse OU não seja utilizado, o mesmo deverá ser grafado com o texto "(EM BRANCO)".

e-CNPJ:

O conteúdo do DN apresenta-se da seguinte forma para os certificados de Pessoa Jurídica (e-CNPJ):

C = BR

O = ICP-Brasil

S = <Sigla da Unidade da Federação>

L = <Cidade>

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-CNPJ A3

OU = <Identificação da AR>

CN = <Nome Empresarial> <:> <número de inscrição no CNPJ>

Onde:

O Common Name (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com cumprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

Campo "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

O campo locality (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.

O campo state or province name (S) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

<u>e-Servidor:</u>

O conteúdo do DN apresenta-se da seguinte forma para os certificados de equipamento Servidores:

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-Servidor A3

OU = <Identificação da AR>
CN = <DNS do Servidor>

Onde:

O "Common Name" (CN) é composto pelo DNS do servidor.
Campo "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

e-Aplicação:

O conteúdo do DN apresenta-se da seguinte forma para os certificados de aplicação:

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-Aplicacao A3

OU = <Identificação da AR>

CN = <Nome da Aplicação> <:> <número de inscrição no CNPJ>

Onde:

O "Common Name" (CN) é composto do nome da aplicação, acrescido do sinal de dois pontos (:) mais o número de inscrição no Cadastro de Pessoas Jurídica (CNPJ).

Campo "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

e-Código:

O conteúdo do DN apresenta-se da seguinte forma para os certificados de assinatura de código de software:

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-Codigo A3

OU = <Identificação da AR>

CN = <Nome Empresarial> <:> <número de inscrição no CNPJ>

Onde:

O "Common Name" (CN) é composto do nome empresarial, acrescido do sinal de dois pontos (:) mais o número de inscrição no Cadastro de Pessoas Jurídica (CNPJ).

Campo "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

7.1.5.Restrições de nome

7.1.5.1. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Imprensa Oficial SP RFB são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

7.1.6.OID (Object Identifier) de Política de Certificado

O OID desta PC é: 2.16.76.1.2.3.6.

Todo certificado emitido segundo essa PC, PC A3 da AC Imprensa Oficial SP RFB, contem o valor desse OID presente na extensão Certificate Policies.

7.1.7.Uso da extensão "Policy Constraints"

Item não aplicável.

7.1.8. Sintaxe e semântica dos qualificadores de política

Os campos **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC Imprensa Oficial SP RFB (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP_RFB/DPC_AC_IMESP_RFB.pdf)

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Imprensa Oficial SP RFB implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC Imprensa Oficial SP RFB e sua criticalidade.

7.2.2.2. As LCR da AC Imprensa Oficial SP RFB obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

a) **"Authority Key Identifier"**: não crítica: contém o hash SHA-1 da chave pública da AC Imprensa Oficial SP RFB.;

b) **"CRL Number"**, não crítica: contém um número seqüencial para cada LCR emitida pela AC Imprensa Oficial SP RFB.

c) **"Authority Information Access"**, não crítica: deve conter somente o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. Não deve ser utilizado nenhum outro método de acesso diferente de id-ad-caIssuer.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC Imprensa Oficial SP RFB. A aprovação e conseqüente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

8.2. Políticas de publicação e notificação

A AC Imprensa Oficial SP RFB mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço *Web*:

(http://icp-brasil.certisign.com.br/repositorio/pc/AC_IMESP_RFB/PC_A3_AC_IMESP_RFB_v6.0.pdf)

8.3. Procedimentos de aprovação

Esta DPC da AC Imprensa Oficial SP RFB foi submetida à aprovação, durante o processo de credenciamento da AC Imprensa Oficial SP RFB, conforme o determinado CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

9. DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio Http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01